Firmware Analysis of Cisco/Linksys SRW2008 - 1.0.4

March 28, 2018

1 Meta Daten

HID	Cisco/Linksys SRW2008 - 1.0.4
Device Name	SRW2008
Vendor	Cisco/Linksys
Device Class	Switch (Managed)
Version	1.0.4
Release Date	2007-09-06
Size	3378139

2 Analysis

2.1 base64decoder

Time of Analysis	2018-03-23 16:12:44
Plugin Version	0.1.2
Summary	

2.2 cpu architecture

Time of Analysis	2018-03-23 16:12:54
Plugin Version	0.3.1
Summary	

2.3 crypto material

Time of Analysis	2018-03-23 16:12:30
Plugin Version	0.5
Summary	

2.4 exploit mitigations

Time of Analysis	2018-03-23 16:12:48
Plugin Version	0.1.1
Summary	

2.5 file hashes

Time of Analysis	2018-03-23 16:12:57
Plugin Version	1.0
imphash	None
sha512	937f575dfffcfe1f986faf4ca8e3ba836f6d6f9dfaab582c4561fa93c7c2b0ceee92efdb3e3e87abe0bbf9a8
ripemd160	5e0313f309e610bece33bfece02a933bb80bc7b9
sha1	5ea563d79a7ed3f8c7a872e0bf31db9ef8c90711
sha256	b7c55a6de9fd1b85ec07f661b4d21638021999e2b1e754de1922f3b01f2cedb8
whirlpool	69477a040d3430dc6706d1bb6a4e2088814e24e6f3d73eb14b2e0e41aee6ba0220d98a4896b872abd5
ssdeep	98304:nNasK108t/KzpM7NURKVt9RMN6sc0KzLgP:nNFK1Dt/KFMX0670KIP
md5	9665a7ad243bda91ce6312ed3aab305d

2.6 file type

Time of Analysis	2018-03-23 16:12:46
Plugin Version	1.0
File Type	ROS Container
MIME	firmware/ros
Summary	firmware/ros

2.7 init systems

Time of Analysis	2018-03-23 16:12:51
Plugin Version	0.4.1
Summary	

2.8 ip and uri finder

Time of Analysis	2018-03-23 16:12:21
Plugin Version	0.4.1
IPv4	1.0.4.1
IPv6	B:: 3:: ::6B ::4 5:: ::c ::D E:: ::9a9 b:: 0:: :: A:: ::7
URI	The List is empty.
Summary	1.0.4.1 B:: 3:: ::6B ::4 5:: ::c ::D E:: ::9a9 b:: 0:: :: A:: ::7

2.9 software components

Time of Analysis	2018-03-23 16:12:33
Plugin Version	0.3
Summary	

2.10 printable strings

<table>
<tr><td>Time of Analysis</td><td>2018-03-23 16:12:27</td></tr>
<tr><td>Plugin Version</td><td>0.2</td></tr>
<tr><td>Strings</td><td>['\t\nX^|v', '\t\x0b?\n1F', '\t\x0bpNRC>', '\t\r1r\\V$_', '\t\r\\h8D', '\t \x0b</td></tr>
</table>

2.11 users and passwords

Time of Analysis	2018-03-23 16:12:40
Plugin Version	0.4
Summary	

2.12 string evaluator

Time of Analysis	2018-03-23 16:12:37
Plugin Version	0.2
Strings	['char OGCFG_link_time[] = " 09:11:40";\r\nchar OGCFG_link_date[] = " 06-Sep-20

2.13 unpacker

Time of Analysis	2018-03-23 16:12:12
Plugin Version	0.7
Plugin	ROSFile
Extracted	6

Output

```

ROS PACK firmware archive payload extractor
Version 0.6
(c) Copyright 2015 TJ <hacker@iam.tj>
Licensed on the terms of the GNU General Public License version 2

Filename:          /media/data/fact_fw_data/b7/b7c55a6de9fd1b85ec07f661b4d21638
File length:       3378139 (0x338bdb)
ARC Magic:         LSS2
ARC Index:         1.01
Header    version: 1
           length: 48
Payload
           length: 3378091 (0x338bab)
         checksum: 430634778 (0x19aaf71a)
Link Time:         09:12:58
Link Date:         2007-09-06
Signature:         PACK
Dir Entries:       6
Extracted CLI_FILE from offset 272 (105518 bytes)
Extracted DELSCRF from offset 105822 (262313 bytes)
Extracted EWS_FILE from offset 368135 (413361 bytes)
Extracted UPNP_FILE from offset 781528 (8407 bytes)
Extracted DATETIME_C from offset 789935 (160 bytes)
Extracted RSCODE from offset 790127 (2588012 bytes)

Payload      length: 3378091 (0x338bab)
Payload   extracted: 3378091 (0x338bab)
Payload    checksum: 430634778 (0x19aaf71a)
Calculated checksum: 430634778 (0x19aaf71a)
```

Size packed unpacked	`3.22 MiB -> 3.22 MiB`
Entropy	0.9
Summary	no data lost

2.14 malware scanner

Time of Analysis	2018-03-23 16:12:23
Plugin Version	0.3
MD5	9665a7ad243bda91ce6312ed3aab305d
System Version	0.2.6
Scanners Number	1
Positives	0
Scanners	ClamAV
Scanns	
	`ClamAV : {'result': 'clean', 'detected': False, 'version': 'ClamAV 0.99.4/24413`
Summary	